UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,202	03/02/2004	Charles J. Stancil	200314559-1	1999

22879 7590 11/21/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
11/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,202	STANCIL, CHARLES J.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 28, 2007. Claims 1-28 were originally received for consideration. No claims were added or cancelled in the received amendment.

2. Claims 1-28 are currently pending consideration.

Response to Arguments

Applicant's arguments filed on September 28, 2007 have been fully considered but they are not persuasive for the following reasons:

Regarding currently amended claim 1, the Applicant argues that the Cited Prior Art (CPA), Stancil et al. (U.S. Patent 6,065,081) in view of Mooney et al. (U.S. Patent 5,515,4440), does not teach a system "configured to receive authorization from a remote network administrator device" to communicatively couple to a connection device with a processing system. The Applicant asserts that there is no remote or separate device which authorizes the coupling of the connection device. This argument is not found persuasive. Stancil discloses a system of disabling and enabling slots which peripheral devices (connection devices) can be communicatively coupled with a processing system based what the administrator designates (Stancil: column 5, lines 10-23). The administrator's machine which does the enabling or disabling of the slots is interpreted as the "remote network administrator device" as it is an administrator device which is in charge of enabling or disabling slots which control the coupling of the

connection devices (Stancil: column 10, lines 15-23). The connection devices are viewed as the local devices, and since the administrator device in Stancil is not the connection device, it is properly interpreted as a "remote device."

Furthermore, in regards to claim 1, the Applicant argues that the CPA does not teach "a card detector configured to detect the presence of the connection device" that "facilitates connectivity between the processing system and a separate processing system or peripheral device." This argument is not found persuasive. Mooney discloses a card reader which "upon a valid security administrator card being placed in a card reader" initializes and authorizes the card (Mooney: column 2, lines 10-15). It is inherent that this is the same as detecting a card. Upon this detection, the CPU turns on power to computer peripherals that the user has been authorized to use (Mooney: column 2, lines 5-8). This is equated to facilitating connectivity with a separate system or device as the peripherals are separate from the processing system.

The Applicant, regarding claim 1, argues that the CPA does not teach "wherein no input from a user of the system is used to determine whether power is to be supplied to the connection device." First, it appears that there is no support for this limitation in the specification. In fact, on page 4, paragraph 20, it states that an owner, network administrator or other authorized individual provides the authorization for a peripheral device to be communicatively coupled to a processing system. The Examiner found no other statements supporting this limitation, and therefore, it is deemed indefinite. Even if there was support for this limitation in the specification, it is asserted that the CPA does teach the limitation. Mooney states that "the user's responses are saved and

compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to the computer peripherals the user has been authorized to use" (Mooney: column 2, lines 4-8). Though based on a user previous responses, the act of supplying power to the peripheral is done automatically based off the card with no user input to the system.

Therefore, the rejection for the claims is maintained and the CPA is applied to the new limitations in the rejection given below.

Claim Rejections - 35 USC § 112

Claims 1-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The independent claims all contain the language of "wherein no input from a user of the system is used to determine whether power is to be supplied to the connection device." First, it appears that there is no support for this limitation in the specification. In fact, on page 4, paragraph 20, it states that an owner, network administrator or other authorized individual provides the authorization for a peripheral device to be communicatively coupled to a processing system. The Examiner found no other statements supporting this limitation, and therefore, it is deemed indefinite.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1,2,4-9,11-15,17,19-23,25, and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stancil et al. (U.S. Patent 6,065,081) in view of Mooney et al. (U.S. Patent 5,515,44).

Regarding claim 1, Stancil discloses:

A system that authorizes connection devices, the system comprising:

a communication system interface (column 5, lines 10-13: "*the user is given the opportunity to enter an administrator password*") configured to receive authorization from a remote network administrator device (column 5, lines 13-16: *if password is entered correctly, the administrator may disable or enable slots*) for a processing system to communicatively couple to an intermediary connection device that facilitates between the processing system and a separate processing system or peripheral device (column 5, lines 17-27), *wherein the slots are disabled or enabled, disabling or enabling the devices connected to those slots* (column 2, lines 63-64).

Stancil does not explicitly disclose a card detector configured to detect the presence of the connection device and a card power switch configured to receive an

authorization signal when the processing system is authorized to coupe to the connection device and configured to apply power to the connection device only when the authorization signal is present and when the card detector detects the presence of the connection device. Stancil also does not explicitly state that no user input is used to determining if power should be supplied to the connection device. Mooney discloses a system that controls access to peripheral devices by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney: column 2, lines 5-8). The CPU and the program logic device (PLD) (card detector) detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized.

The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. Mooney also teaches that no input from a user is used to determine whether power is to be supplied to the connection device. Mooney states that "the user's responses are saved and compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to the computer peripherals the user has been authorized to use" (Mooney: column 2, lines 4-8). Though based on a user previous responses, the act of supplying power to the peripheral is done automatically based off the card with no user input to the system. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Stancil discloses:

The system of claim 1, further comprising an input/output (I/O) connection configured to couple to the connection device such that the communications can be received via the connection device from another communication system or a peripheral device (column 5, lines 17-24), *wherein enabled slots will allow peripheral devices to*

communicate with the computer system, wherein the peripheral devices can include a modem (column 1, lines 13-15) which can communicate with another communication system.

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Stancil discloses:

The system of claim 2, wherein the I/O connection comprises a Peripheral Component Interconnect (PCI) Express connection (column 1, lines 51-53), *wherein the add-in card slots can e PCI or ISA.*

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Stancil discloses:

The system of claim 2, wherein the I/O connection comprises an Industry Standard Architecture (ISA) connection (column 1, lines 51-53), *wherein the add-in card slots can e PCI or ISA.*

Claim 6 is rejected as applied above in rejecting claim 1. Stancil does not explicitly teach a connection to the card detector such that the card detector communicates the authorization signal to the card power switch. The system of Stancil-Mooney, as described in rejecting claim 1, teaches a connection to the card detector such that the card detector communicates the authorization signal to the card power switch. The Stancil-Mooney system contains a CPU and a program logic device (PLD) (card

detector) to detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). This configuration sends the authorization signal from the CPU to the PLD/ASIC (card detector) and to the card power switch. Therefore, the system of Stancil-Mooney does teach communicating the authorization signal to the card power switch through the card detector. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 7 is rejected as applied above in rejecting claim 1. Stancil does not explicitly disclose a connection to the card power switch from a communication bus such that the authorization signal is received by the card power switch. Mooney teaches that the peripherals are controlled by the CPU and the PLD (card detector) by using a power control circuit (column 4, lines 23-28), wherein the CPU and the PLD communicate the authorization signal via a system data bus (Mooney: column 4, lines 25-29) to the power control switch, which turns on/off the peripherals. This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and

the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Stancil teaches:

a memory configured to store the authorization from the network administrator device (column 5, lines 17-20), *wherein the slots are disabled/enabled according to the configuration stored in the non-volatile memory*;

Stancil does not explicitly teach a processor configured to retrieve the authorization from the memory and further configured to cause the authorization signal to be communicated to the card power switch. Mooney teaches a microprocessor compares the user response to a response stored on a card (memory) and returns a compare status to the CPU (processor) (column 5, lines 57-61) and turns on/off the power to the peripherals by way of an authorization signal sent to through the CPU and the PLD to the peripherals (column 4, lines 23-28). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an

authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Stancil discloses:

The system of claim 1, further comprising a single receptacle residing on the processing system, wherein the connection device and a second type of connection device are configured to couple to the processing system using the single receptacle (column 1, lines 13-16), *wherein network cards, modems, and other devices can be removed and added.*

Claim 11 is rejected as applied above in rejecting claim 9. Furthermore, Stancil discloses:

The system of claim 9, further comprising:

a signal generator configured to generate the authorization signal (column 4, lines 51-61), *wherein an administrator disables/enables a slot which generates a disable or enable signal*;

a logical OR gate (column 4, lines 51-54: "logical OR") comprising:

a first input coupled to the signal generator (Figure 4, column 4 lines 53-61), *wherein an signal is input to the OR gate.*

Stancil does not explicitly disclose a card detector configured to detect the presence of the connection device and a card power switch configured to receive an authorization signal when the processing system is authorized to coupe to the connection device and configured to apply power to the connection device only when the authorization signal is present and when the card detector detects the presence of the connection device. Stancil also does not explicitly state that no user input is used to determining if power should be supplied to the connection device. Mooney discloses a system that controls access to peripheral devices by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney: column 2, lines 5-8). The CPU and the program logic device (PLD)

(card detector) detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. Mooney also teaches that no input from a user is used to determine whether power is to be supplied to the connection device. Mooney states that "the user's responses are saved and compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to the computer peripherals the user has been authorized to use" (Mooney: column 2, lines 4-8). Though based on a user previous responses, the act of supplying power to the peripheral is done automatically based off the card with no user input to the system. It

would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 12 is rejected as applied above in rejecting claim 1. Stancil does not explicitly a violation detector configured to detect presence of the connection device and further configured to communicate a violation signal to the network administrator device when the connection device is not authorized to be communicatively coupled to the processing system. Mooney teaches a violation detector which communicates a violation signal to the network administrator when the connection device is not authorized to be communicatively coupled to the processing system (Mooney: column 5, lines 57-65). Mooney teaches that a microprocessor (violation detector) compares user input to a response stored in memory (column 5, lines 57-60) and returns a compare status to CPU (column 5, line 60). This result could be one of a matching response or a non-matching response (violation signal) (column 5, lines 61-64). Mooney uses this violation detector in order to alert the system administrator in case the system administrator wants to take corrective action (column 6, lines 1-3). . It would have been obvious to one of ordinary skill in the art at the time of invention to use the violation detector as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still

maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Regarding claim 13, Stancil discloses:

A method for authorizing connection devices, the method comprising:

detecting the presence of an intermediary connection device when coupled to a processing system, the connection device being configured to facilitate connectivity between the processing system and a separate processing system or peripheral device (column 3, lines 23-25), *wherein the ASIC is able to disable/enable slots which it detects*.

Stancil does not explicitly disclose determining if the connection device is authorized to be communicatively coupled to the processing system and providing power to the connection device when it is authorized and not providing power to the connection device if the connection device is not authorized. Mooney discloses a system that controls access to peripheral devices by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney: column 2, lines 5-8). The CPU and the program logic device (PLD) (card detector) detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4,

lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Stancil discloses:

The method of claim 13, further comprising receiving an authorization from a remote administrator device via a communication system (column 5, lines 13-16: *if password is entered correctly, the administrator may disable or enable slots*) coupling the remote network administrator device and the processing system (column 5, lines 13-16), *wherein if password is entered correctly, the administrator may disable or enable slots*).

Claim 15 is rejected as applied above in rejecting claim 13. Stancil does not explicitly teach generating an authorization signal when the connection device is authorized to be communicatively coupled and communicating the authorization signal to a card power switch such that the card power switch provides power to the connection device. The system of Stancil-Mooney, as described in rejecting claim 1, teaches a connection to the card detector such that the card detector communicates the authorization signal to the card power switch. The Stancil-Mooney system contains a CPU and a program logic device (PLD) (card detector) to detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). This configuration sends the authorization signal from the CPU to the PLD/ASIC (card detector) and to the card power switch. Therefore, the system of Stancil-Mooney does teach communicating the authorization signal to the card power switch through the card detector. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the

system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Stancil discloses:

The method of claim 13, further comprising:

detecting presence of a second type of connection device when coupled to the processing system (column 3, lines 23-25), *wherein the ASIC is able to disable/enable slots which it detects and can be one of many different devices (column 1, lines 13-15).*

Stancil does not explicitly disclose determining if the second type of connection device is authorized to be communicatively coupled to the processing system and providing power to the second type of connection device when it is authorized and not providing power to the second type of connection device if the second type of connection device is not authorized. Mooney discloses a system that controls access to peripheral devices (can be either first or second type) by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney: column 2, lines 5-8). The CPU and the program logic device (PLD) (card detector) detect and control the peripherals within the computer and turn on/off

power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 19 is rejected as applied above in rejecting claim 13. Furthermore, Stancil discloses:

The method of claim 13, wherein the connection device and the second type of connection device are configured to couple to the processing system using a single receptacle residing on the processing system (column 1, lines 13-16), *wherein network cards, modems, and other devices can be removed and added.*

Claim 20 is rejected as applied above in rejecting claim 13. Stancil does not explicitly a violation detector configured to detect presence of the connection device and further configured to communicate a violation signal to the network administrator device when the connection device is not authorized to be communicatively coupled to the processing system. Mooney teaches a violation detector which communicates a violation signal to the network administrator when the connection device is not authorized to be communicatively coupled to the processing system (Mooney: column 5, lines 57-65). Mooney teaches that a microprocessor (violation detector) compares user input to a response stored in memory (column 5, lines 57-60) and returns a compare status to CPU (column 5, line 60). This result could be one of a matching response or a non-matching response (violation signal) (column 5, lines 61-64). Mooney uses this violation detector in order to alert the system administrator in case the system administrator wants to take corrective action (column 6, lines 1-3). . It would have been obvious to one of ordinary skill in the art at the time of invention to use the violation detector as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still

maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Regarding claim 21, Stancil discloses:

A system for authorizing connection devices, the system comprising:

means for detecting presence of an intermediary connection device when coupled to a processing system, the connection device being configured to facilitate connectivity between the processing system and a separate processing system or peripheral device (column 3, lines 23-25), *wherein the ASIC is able to disable/enable slots which it detects and can be one of many different devices (column 1, lines 13-15).*

Stancil does not explicitly disclose a card detector configured to detect the presence of the connection device and a card power switch configured to receive an authorization signal when the processing system is authorized to coupe to the connection device and configured to apply power to the connection device only when the authorization signal is present and when the card detector detects the presence of the connection device. Stancil also does not explicitly state that no user input is used to determining if power should be supplied to the connection device. Mooney discloses a system that controls access to peripheral devices by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney:

column 2, lines 5-8). The CPU and the program logic device (PLD) (card detector) detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. Mooney also teaches that no input from a user is used to determine whether power is to be supplied to the connection device. Mooney states that "the user's responses are saved and compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to the computer peripherals the user has been authorized to use" (Mooney: column 2, lines 4-8). Though based on a user previous responses, the act of supplying power to the peripheral is done automatically based off the card

with no user input to the system. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Stancil discloses:

The system of claim 21, further comprising means for receiving an authorization from a remote network administrator device via a communication system coupling the remote network administrator device and the processing system (column 5, lines 13-16: *if password is entered correctly, the administrator may disable or enable slots*) coupling the remote network administrator device and the processing system (column 5, lines 13-16), *wherein if password is entered correctly, the administrator may disable or enable slots*).

Claim 23 is rejected as applied above in rejecting claim 21. Stancil does not explicitly teach generating an authorization signal when the connection device is authorized to be communicatively coupled and communicating the authorization signal to a card power switch such that the card power switch provides power to the connection device. The system of Stancil-Mooney, as described in rejecting claim 1, teaches a connection to

the card detector such that the card detector communicates the authorization signal to the card power switch. The Stancil-Mooney system contains a CPU and a program logic device (PLD) (card detector) to detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). This configuration sends the authorization signal from the CPU to the PLD/ASIC (card detector) and to the card power switch. Therefore, the system of Stancil-Mooney does teach communicating the authorization signal to the card power switch through the card detector. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 25 is rejected as applied above in rejecting claim 21. Furthermore, Stancil discloses:

The method of claim 21, further comprising:

means for detecting presence of a second type of connection device when coupled to the processing system (column 3, lines 23-25), *wherein the ASIC is able to disable/enable slots which it detects and can be one of many different devices (column 1, lines 13-15).*

Stancil does not explicitly disclose means for determining if the second type of connection device is authorized to be communicatively coupled to the processing system and providing power to the second type of connection device when it is authorized and not providing power to the second type of connection device if the second type of connection device is not authorized. Mooney discloses a system that controls access to peripheral devices (can be either first or second type) by using a system administrator card to authorize other user cards (Mooney: column 2, lines 9-15). If the user card is authorized, a power control circuit (card power switch) is used by the CPU to turn on power to computer peripherals (connection devices) that the user has been authorized to use (Mooney: column 2, lines 5-8). The CPU and the program logic device (PLD) (card detector) detect and control the peripherals within the computer and turn on/off power to the detected peripherals using the power control circuit (Mooney: column 4, lines 20-26). As mentioned earlier, the power control circuit (card power switch) only supplies power to the connection device it is authorized (authorization signal is present) and when there is a peripheral that is connected according to the CPU and the PLD (card detector) (Mooney: column 6, lines 4-6). Stancil and Mooney are analogous arts because they both provide methods of disabling peripheral devices connected to a computer system if authorized by a system administrator. Mooney uses an authorization procedure using a card and a card reader, and then supplies power to the peripherals only if the user is authorized (Mooney: column 2, lines 5-8). This authorization system of Mooney could be implemented in the system of Stancil to automatically disable (not supply power to) the peripherals which

are not authorized. The power control circuit of Mooney could be connected between the ASIC (analogous to the PLD of Mooney) and the ISA/PCI clots (Stancil: Figure 2) to allow/disallow the power to be supplied to the peripherals based on the authorization signal. It would have been obvious to one of ordinary skill in the art at the time of invention to use the card power switch to supply power only if an authorization signal is received as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

Claim 27 is rejected as applied above in rejecting claim 21. Furthermore, Stancil discloses:

The system of claim 21, further comprising means for coupling the connection device and the second type of connection device to the processing system using the same means for coupling residing on the processing system (column 1, lines 13-16), *wherein network cards, modems, and other devices can be removed and added.*

Claim 28 is rejected as applied above in rejecting claim 21. Stancil does not explicitly a means for determining that the connection is not authorized and further means for generating a violation signal and means for communicating the violation signal to the network administrator device when the connection device is not authorized to be communicatively coupled to the processing system. Mooney teaches a violation detector which communicates a violation signal to the network administrator when the

connection device is not authorized to be communicatively coupled to the processing system (Mooney: column 5, lines 57-65). Mooney teaches that a microprocessor (violation detector) compares user input to a response stored in memory (column 5, lines 57-60) and returns a compare status to CPU (column 5, line 60). This result could be one of a matching response or a non-matching response (violation signal) (column 5, lines 61-64). Mooney uses this violation detector in order to alert the system administrator in case the system administrator wants to take corrective action (column 6, lines 1-3). . It would have been obvious to one of ordinary skill in the art at the time of invention to use the violation detector as disclosed by Mooney in the system of Stancil "to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system" (Mooney: column 1, lines 48-52).

8. Claims 3, 10, 16, 18, 24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stancil et al. (U.S. Patent 6,065,081) in view of Mooney et al. (U.S. Patent 5,515,44) in further in view of Morrow (U.S. Patent Pub. No. US 2004/0156151).

Claim 3 is rejected as applied above in rejecting claim 2. Stancil and Mooney do not explicitly disclose that the I/O connection comprises a Universal Serial Bus (USB) connection. Stancil discloses a system and method for disabling add-in card slots (e.g. PCI or ISA) in a computer system (column 1, lines 51-53), but does not explicitly mention the use of a USB connection. Morrow discloses a system of detecting and

powering a USB PC card (paragraph 10: lines 1-4). Morrow is analogous to Stancil and Morrow as all three deal with providing power/enabling PC cards. Morrow uses the USB as the preferred embodiment for the invention because USB is the "most popular of these serial bus technologies" (Morrow: paragraph 0007: lines 1-4) and it can provide "400+ million bits per second throughput" (Morrow: paragraph 007: lines 5-6). The system of Stancil-Mooney could be modified to support USB cards, as the power would still be provided by way of a card power switch (as disclosed in Mooney and Morrow) and connection to the card slot would remain the same. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the system of Stancil-Mooney to support the USB connection as disclosed by Morrow, because USB is the "most popular of these serial bus technologies" (Morrow: paragraph 0007: lines 1-4) and it can provide "400+ million bits per second throughput" (Morrow: paragraph 007: lines 5-6).

Claim 10 is rejected as applied above in rejecting claim 9. The system of Stancil and Mooney does not explicitly teach that the card power switch provides a first power that is unique to power requirements of the connection device and a second power that is unique to the power requirements of the second device. Morrow discloses a card power switch which includes a card sense block that detects type of PC card is being installed in a slot and provides the correct voltage depending on the type of card (Morrow: paragraph 0059: lines 1-9). Morrow is analogous to Stancil and Morrow as all three deal with providing power/enabling PC cards. Morrow uses the power sensing block so

that the controller "enables the appropriate electrical interface to the card, and communicates via electrical control signals to the PC Card Power Switch indicating the voltage requirements of the card" (Morrow: paragraph 0004, lines 6-12). The card sensing block could be incorporated into the card power switch (Mooney: Figure 2, item 119) of Stancil-Mooney so that the correct voltage can be detected. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the card sensing block of Morrow, so that the correct voltage could be provided to the card, depending on the type of card (Morrow: paragraph 0004, lines 6-12).

Claim 16 is rejected as applied above in rejecting claim 13. The system of Stancil and Mooney does not explicitly teach that the card power switch provides power that is unique to the power requirements of the connection device. Morrow discloses a card power switch which includes a card sense block that detects type of PC card is being installed in a slot and provides the correct voltage depending on the type of card (Morrow: paragraph 0059: lines 1-9). Morrow is analogous to Stancil and Morrow as all three deal with providing power/enabling PC cards. Morrow uses the power sensing block so that the controller "enables the appropriate electrical interface to the card, and communicates via electrical control signals to the PC Card Power Switch indicating the voltage requirements of the card" (Morrow: paragraph 0004, lines 6-12). The card sensing block could be incorporated into the card power switch (Mooney: Figure 2, item 119) of Stancil-Mooney so that the correct voltage can be detected. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the

card sensing block of Morrow, so that the correct voltage could be provided to the card, depending on the type of card (Morrow: paragraph 0004, lines 6-12).

Claim 18 is rejected as applied above in rejecting claim 17. The system of Stancil and Mooney does not explicitly teach that the card power switch provides power that is unique to the power requirements of the second type of connection device. Morrow discloses a card power switch which includes a card sense block that detects type of PC card is being installed in a slot and provides the correct voltage depending on the type of card (Morrow: paragraph 0059: lines 1-9). Morrow is analogous to Stancil and Morrow as all three deal with providing power/enabling PC cards. Morrow uses the power sensing block so that the controller "enables the appropriate electrical interface to the card, and communicates via electrical control signals to the PC Card Power Switch indicating the voltage requirements of the card" (Morrow: paragraph 0004, lines 6-12). The card sensing block could be incorporated into the card power switch (Mooney: Figure 2, item 119) of Stancil-Mooney so that the correct voltage can be detected. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the card sensing block of Morrow, so that the correct voltage could be provided to the card, depending on the type of card (Morrow: paragraph 0004, lines 6-12).

Claim 24 is rejected as applied above in rejecting claim 21. The system of Stancil and Mooney does not explicitly teach that the card power switch provides power that is unique to the power requirements of the connection device. Morrow discloses a card power switch which includes a card sense block that detects type of PC card is being installed in a slot and provides the correct voltage depending on the type of card (Morrow: paragraph 0059: lines 1-9). Morrow is analogous to Stancil and Morrow as all three deal with providing power/enabling PC cards. Morrow uses the power sensing block so that the controller "enables the appropriate electrical interface to the card, and communicates via electrical control signals to the PC Card Power Switch indicating the voltage requirements of the card" (Morrow: paragraph 0004, lines 6-12). The card sensing block could be incorporated into the card power switch (Mooney: Figure 2, item 119) of Stancil-Mooney so that the correct voltage can be detected. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the card sensing block of Morrow, so that the correct voltage could be provided to the card, depending on the type of card (Morrow: paragraph 0004, lines 6-12).

Claim 26 is rejected as applied above in rejecting claim 25. The system of Stancil and Mooney does not explicitly teach that the card power switch provides power that is unique to the power requirements of the second type of connection device. Morrow discloses a card power switch which includes a card sense block that detects type of PC card is being installed in a slot and provides the correct voltage depending on the type of card (Morrow: paragraph 0059: lines 1-9). Morrow is analogous to Stancil and

Morrow as all three deal with providing power/enabling PC cards. Morrow uses the power sensing block so that the controller "enables the appropriate electrical interface to the card, and communicates via electrical control signals to the PC Card Power Switch indicating the voltage requirements of the card" (Morrow: paragraph 0004, lines 6-12). The card sensing block could be incorporated into the card power switch (Mooney: Figure 2, item 119) of Stancil-Mooney so that the correct voltage can be detected. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the card sensing block of Morrow, so that the correct voltage could be provided to the card, depending on the type of card (Morrow: paragraph 0004, lines 6-12).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA. 11/17/07

KA
11/17/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100